Having thus described the invention, it is claimed:

1. A method of reducing handoff latency of a mobile node MN roaming between access points in a wireless network WLAN, the method comprising:

authenticating the mobile node MN with an access point AP to produce a pairwise master key PMK;

establishing a pairwise transient key PTK as a link layer session key to provide secure communication of 802.1X messages and 802.11 data between the mobile node MN and the access point AP; and,

associating the mobile node MN with the access point AP in said wireless network WLAN.

2. The method according to claim 1 wherein said authenticating and said establishing are initiated before said re-associating.

3. The method according to claim 1 wherein said establishing establishes said pairwise transient key PTK before said associating is initiated.

4. The method according to claim 3 wherein said associating includes issuing an association request by said mobile node MN to the access point AP including signature information indicative of the mobile node MN holding a fresh/live pairwise transient key PTK.

5. The method according to claim 4 further including:

validating the signature information by the access point AP; and,

delivering a protected group transient key GTK from the mobile node MN to the access point AP, the group transient key being used to protect broadcast communication of the access point AP, generating an association response to send to the STA containing an encrypted field protecting the GTK and including signature information indicative of the AP holding the same fresh/live key PTK as the STA.

6. The method according to claim 5 further including:

validating the signature information by the STA and storing the encrypted GTK for use in multicast communications by the AP; and

forwarding a re-association confirmation message from the mobile node MN to the access point AP to confirm receipt of the group transient key GTK by the mobile node MN.

7. The method according to claim 6 wherein:

said issuing the re-association request by the mobile node MN includes issuing a resuscitation request as Authenticate PTK (SRandom, PTKID MIC);

said validating and said delivering includes delivering a re-association response from the access point AP to the mobile node MN as Authenticate PTK (ARandom, SRandom, PTKID, GTK, GTKID, MIC), deliver encrypted group key; and,

said forwarding the re-association confirmation message includes forwarding a re-association confirm from the mobile node MN to the access point AP as Group Key Confirm (ARandom, MIC).

8. The method according to claim 3 wherein said establishing includes performing an 802.11 4-way handshake to generate said pairwise transient key PMK using said pairwise master key PMK.

9. The method according to claim 3 wherein the authenticating includes:

producing said pairwise master key PMK by at least one of:

retrieving said pairwise master key PMK from a cache memory of said access point AP, and

executing an 802.1X extensible authenticated protocol EAP by the access point AP together with an authentication server AS of said wireless network WLAN to generate said pairwise master key PMK.

10. The method according to claim 1 wherein said authenticating includes negotiating a security association type.

11. In a wireless network WLAN including at least one mobile node MN roaming between access points of the wireless network WLAN, a system for reducing handoff latency, the system comprising:

means for authenticating the mobile node MN with an access point AP to produce a pairwise master key PMK;

means for establishing a pairwise transient key PTK as a link layer session key to provide secure communication of 802.1X messages and 802.11 data between the mobile node MN and the access point AP; and,

means for associating the mobile node MN with the access point AP in said wireless network WLAN.

12. The system according to claim 11 wherein said means for authenticating and said means for establishing are initiated before said means for re-associating.

13. The system according to claim 11 wherein said means for establishing is adapted to establish said pairwise transient key PTK before said associating means is initiated.

14. The system according to claim 13 wherein said re-associating means includes means for issuing a re-association request by said mobile node MN to the access point AP including signature information indicative of the mobile node MN holding a fresh/live pairwise transient key PTK.

15. The system according to claim 14 further including:

means for validating the signature information by the access point AP; and,

means for delivering a protected group transient key GTK from the mobile node MN to the access point AP, the group transient key being used to protect broadcast traffic from the access point AP, generating an association response to send to the STA containing an encrypted field protecting the GTK and including signature information indicative of the AP holding the same fresh/live key PTK as the STA.

16. The system method according to claim 15 further including:

validating the signature information by the STA and storing the encrypted GTK for use in multicast communications by the AP; and

means for forwarding a re-association confirmation message from the mobile node MN to the access point AP to confirm receipt of the group transient key GTK by the mobile node MN.

17. The system according to claim 16 wherein:

said means for issuing the re-association request by the mobile node MN includes means for issuing a resuscitation request as Authenticate PTK (SRandom, PTKID MIC);

said means for validating and said delivering includes means for delivering a re-association response from the access point AP to the mobile node MN as Authenticate PTK (ARandom, SRandom, PTKID, GTKID, GTK, MIC), deliver encrypted group key; and,

said means for forwarding the re-association confirmation message includes means for forwarding a re-association confirm from the mobile node MN to the access point AP as Group Key Confirm (ARandom, MIC).

18. The system according to claim 13 wherein said means for establishing includes means for performing an 802.11 4-way handshake to generate said pairwise transient key PMK using said pairwise master key PMK.

19. The system according to claim 13 wherein the means for authenticating includes:

means for producing said pairwise master key PMK by at least one of:

retrieving said pairwise master key PMK from a cache memory of said access point AP, and

executing an 802.1X extensible authenticated protocol EAP by the access point AP together with an authentication server AS of said wireless network WLAN to generate said pairwise master key PMK.

20. The system according to claim 11 wherein said means for authenticating includes means for negotiating a security association type.

21. An article of manufacture comprising a program storage medium readable by a computer and embodying one or more instructions executable by the computer to perform method steps for executing a command to perform method of reducing handoff latency of a mobile node MN roaming between access points in a wireless network WLAN, the method comprising:

authenticating the mobile node MN with an access point AP to produce a pairwise master key PMK;

establishing a pairwise transient key PTK as a link layer session key to provide secure communication of 802.1X messages and 802.11 data between the mobile node MN and the access point AP; and,

associating the mobile node MN with the access point AP in said wireless network WLAN.

22. The article of manufacture according to claim 21 wherein said authenticating and said establishing are initiated before said re-associating.

23. The article of manufacture according to claim 21 wherein said establishing establishes said pairwise transient key PTK before said associating is initiated.

24. The article of manufacture according to claim 23 wherein said re-associating includes issuing a re-association request by said mobile node MN to the access point AP including signature information indicative of the mobile node MN holding a fresh/live pairwise transient key PTK.

25. The article of manufacture according to claim 24 further including:

validating the signature information by the access point AP; and,

delivering a protected group transient key GTK from the mobile node MN to the access point AP, the group transient key being used to protect communication between the mobile node MN, the access point AP, generating an association response to send to the STA containing an encrypted field protecting the GTK and including signature information indicative of the AP holding the same fresh/live key PTK as the STA.

26. The article of manufacture according to claim 25 further including:

validating the signature information by the STA and storing the encrypted GTK for use in multicast communications by the AP; and

forwarding a re-association confirmation message from the mobile node MN to the access point AP to confirm receipt of the group transient key GTK by the mobile node MN.

27. The article of manufacture according to claim 26 wherein:

said issuing the re-association request by the mobile node MN includes issuing a resuscitation request as Authenticate PTK (SRandom, PTKID, MIC);

said validating and said delivering includes delivering a re-association response from the access point AP to the mobile node MN as Authenticate PTK (ARandom, SRandom, PTKID, GTKID, GTK, MIC), deliver encrypted group key; and,

said forwarding the re-association confirmation message includes forwarding a re-association confirm from the mobile node MN to the access point AP as Group Key Confirm (ARandom, MIC).

28. The article of manufacture according to claim 23 wherein said establishing includes performing an 802.11 4-way handshake to generate said pairwise transient key PMK using said pairwise master key PMK.

29. The article of manufacture according to claim 23 wherein the authenticating includes:

producing said pairwise master key PMK by at least one of:

retrieving said pairwise master key PMK from a cache memory of said access point AP, and

executing an 802.1X extensible authenticated protocol EAP by the access point AP together with an authentication server AS of said wireless network WLAN to generate said pairwise master key PMK.

30. The article of manufacture according to claim 21 wherein said authenticating includes negotiating a security association type.